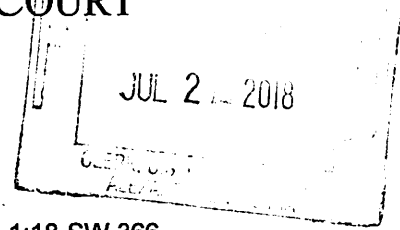


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Content of, and records relating to, e-mail accounts:
george.nadirs@gmail.com, Maintained by Google, Inc.,
Headquartered at 1600 Amphitheatre, Parkway,
Mountain View, CA 94043

Case No. 1:18-SW-366

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. §§ 2252(a)(1); 2252(a)(2) and
 (b)(1); 2252(a)(4)(B) and (b)(2); 2252A(a)(1)
 and (b)(1); 2252A(a)(2)(A) and (b)(1);
 2252A(a)(5)(B) and (b)(2)

Offense Description

Transportation of visual depictions of minors engaged in sexually explicit conduct; receipt and distribution of visual depictions of minors engaged in sexually explicit conduct; Possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct; Transportation of child pornography; Distribution and receipt of child pornography; Possession of and access with intent to view child pornography

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by
 AUSA Laura Fong

Applicant's signature

Special Agent Ted P. Delacourt, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 7/2/18

/s/
 Theresa Carroll Buchanan
 United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF THE ITEMS TO BE SEARCHED

This warrant applies to information associated with the account
george.nadirs@gmail.com which is stored at premises owned, maintained, controlled, or
operated by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway
Mountain View, CA 94043.

ATTACHMENT B

Items to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A:

- a. The contents of all e-mails stored in the accounts (including attachments), including copies of e-mails sent to and from the accounts, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. Any deleted emails, including any information described in subparagraph “a,” above;
- c. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, accounts’ status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. All records or other information stored by the accounts, including but not limited to , push tokens, chat logs, address books, contact and buddy lists, calendar data, pictures, videos and files;
- e. The content of any and all cloud storage accounts;

- f. All records pertaining to Google Voice transactions/calls;
- g. All records pertaining to communications between Google and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

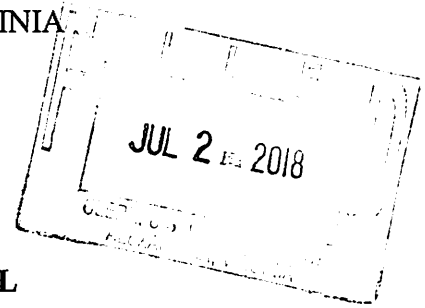
1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1) and (b)(1) (transportation of visual depictions of minors engaged in sexually explicit conduct); 2252(a)(2) and (b)(1) (receipt and distribution of visual depictions of minors engaged in sexually explicit conduct); 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 2252A(a)(1) and (b)(1) (transportation of child pornography); 2252A(a)(2)(A) and (b)(1) (distribution and receipt of child pornography); and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Any and all data, records, communications or information reflecting evidence, fruits, instrumentalities, and contraband of the crimes listed above;
- b. Credit card and other financial information including but not limited to bills and payment records;
- c. Evidence of who used, owned, or controlled the accounts or identifiers listed on Attachment A;
- d. Evidence of the times the accounts or identifiers listed on Attachment A was used;

- e. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN RE SEARCH OF:

Content of, and records relating to,
e-mail accounts:

george.nadirs@gmail.com

Maintained by Google, Inc.,

Headquartered at 1600 Amphitheatre
Parkway, Mountain View, CA 94043

)
)
) **UNDER SEAL**
)
)

)
)
) **CRIMINAL NO. 1:18-SW-366**
)

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Ted P. Delacourt, a Special Agent with the Federal Bureau of Investigation (FBI), Washington Field Division, Washington, D.C., being duly sworn, depose and state as follows:

INTRODUCTION

1. Your Affiant has been employed the FBI since September of 2004, and as a Special Agent since September 2005. Since 2005, I have received training and experience in interviewing and interrogation techniques, and arrest and search procedures. I was assigned as a Special Agent in the Jacksonville Division in January 2006, where I worked counterterrorism and intelligence-gathering operations for approximately three years. I was assigned to the Washington Field Office in May 2009 and charged with investigating international corruption, specifically violations of the Foreign Corrupt Practices Act (FCPA), as well as antitrust violations. In January 2009, I was promoted to Supervisory Special Agent and assigned to the Counterterrorism Division of FBI Headquarters, specifically to the National Joint Terrorism Task Force. In August 2012, I transferred within the Counterterrorism Division to the International

Operations Section I, Continental US Unit V, where I managed International Terrorism investigations in the Phoenix Division. I am currently assigned to the Washington Field Office, Northern Virginia Resident Agency, Child Exploitation Task Force. Since joining the FBI, I have investigated violations of federal law. As a federal agent, I am authorized to investigate violation of laws of the United States and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States. Since September 2014, I have been assigned to investigate violations of law concerning the sexual exploitation of children, including child pornography and child sex trafficking. I have gained experience through both formal and on-the-job training in conducting these types of investigations.

2. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, which included conversations with law enforcement officers and others and review of reports and database records.

3. This Affidavit is made in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by (hereinafter, collectively, "Communication Account Providers"), more fully described in Attachment A:

- a. george.nadirs@gmail.com which is stored at premises owned, maintained, controlled, or operated by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway Mountain view, CA 94043;

4. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Communication Account provider, specified in Attachment A, to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the listed accounts

described in Attachment A, included in the contents of communications. As to the accounts, the evidence and information to be searched is described in the following paragraphs and in Attachments A and B, and there is probable cause to believe that the accounts constitute and/or contain evidence, fruits, contraband, instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1) and (b)(1) (transportation of visual depictions of minors engaged in sexually explicit conduct); 2252(a)(2) and (b)(1) (receipt and distribution of visual depictions of minors engaged in sexually explicit conduct); 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 2252A(a)(1) and (b)(1) (transportation of child pornography); 2252A(a)(2)(A) and (b)(1) (distribution and receipt of child pornography); and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography).

5. The information in this Affidavit is based on my investigation, training, knowledge, and experience, and through information that has been related to me through data, reports and other officers or agents involved in this investigation and related subject area.

6. This Affidavit contains information necessary to support probable cause for this Application. It is not intended to include each and every fact and matter observed by me, other law enforcement officers, or known to the government. Not every fact known to this investigation or by the government is set forth in this Affidavit. Additionally, unless otherwise noted, wherever in this Affidavit I assert that a statement was made by an individual, that statement is described in substance, and in part, and is not intended to be a verbatim recitation of the entire statement.

RELEVANT FEDERAL CRIMINAL STATUTES

7. Title 18, United States Code, Section 2252(a)(1) and (b)(1) prohibits the knowing transportation or shipment of any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or in or affecting interstate commerce by any means, including by computer.

8. Title 18, United States Code, Section 2252(a)(2) and (b)(1) prohibits the knowing receipt or distribution of any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in or affecting interstate or foreign commerce, by any means, including by computer.

9. Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) prohibits the possession of one or more books, magazines, periodicals, films, or other materials which contain any visual depictions of minors engaged in sexually explicit conduct that have been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce, by any means, including by computer.

10. Title 18, United States Code, Section 2252A(a)(1) and (b)(1) prohibits the knowing mailing, or transportation or shipment using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, of any child pornography.

11. Title 18, United States Code, Section 2252A(a)(2) and (b)(1) prohibits the knowing receipt or distribution of any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

12. Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2) prohibits the knowing possession of any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

Google, Inc.

13. The Google Email Premises are email accounts which are hosted by Google, Inc. (hereinafter “the email provider”). In my training and experience, I have learned that email providers provide a variety of on-line services, including email access, to the general public. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with the email provider. During the registration process, the email provider asks subscribers to provide basic personal information. Therefore, the computers of the email provider are likely to contain stored electronic communications (including retrieved and retrieved email for the email provider’s subscribers) and information concerning subscribers and their use of the email provider’s services, such as account access information, the email transaction information, and account application information.

14. In general, an email that is sent to the email provider’s subscriber is stored in the subscriber’s “mail box” on the email provider’s servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the email provider’s servers indefinitely.

15. When the subscriber sends an email, it is initiated at the user’s computer,

transferred via the Internet to the email provider's servers, and then transmitted to its end destination. The email provider often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the email provider's server, the email can remain on the system indefinitely.

16. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by the email provider but may not include all of these categories of data.

17. A subscriber of the email provider can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by the email provider.

18. In my experience, subscribers do not routinely copy emails stored in their email account in order to store the emails on a home computer or other location, although it is possible to do so. This is particularly true when they access their email account through the web, or if they do not wish to maintain particular emails or files in their residence.

19. In general, email providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

20. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the

types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the email provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

21. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

22. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files. Often online bills and other receipts will be sent to an email account, providing further user attribution evidence tied to the account and demonstrating who is ultimately committing the crimes under investigation.

DEFINITIONS

23. The following definitions apply to this Affidavit and its Attachments:

24. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation.

This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

25. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

26. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

27. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

28. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

29. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a

range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

30. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

31. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

32. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

33. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,
THE INTERNET, AND EMAIL**

34. I have had training in the investigation of computer-related crimes and I have consulted more senior law enforcement agents on this matter. Based on my training, experience, and knowledge, I know the following:

35. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve

four functions in connection with child pornography: production, communication, distribution, and storage.

36. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

37. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), cloud storage, and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

38. The Internet affords individuals numerous venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

39. Individuals also use online resources to trade, distribute, store, and retrieve child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet.

UNDERLYING INVESTIGATION

40. GEORGE AREF NADER (hereinafter, "NADER") is a citizen of the United States and Lebanon. On February 27, 1991, NADER was indicted in the Eastern District of Virginia for violations related to smuggling child pornography, Title 18, United States Code, Section 2252(a)(1), by a federal grand jury. The indictment resulted from a seizure of child pornography at the Washington-Dulles International Airport on July 26, 1990 of two reels of video tape concealed in candy tins. On May 6, 1991, NADER pled guilty to a single count of Title 18, Section 2252(a)(1) (transportation of child pornography).

41. On January 16, 2018, Search Warrant 1:18-SW-30 was sworn out in the United States District Court for the Eastern District of Virginia and signed by U.S. Magistrate Judge Ivan D. Davis. The search warrant pertained to a matter unrelated to child pornography. The attachments to the search warrant specified the items to be searched as "the person of George Nader" and "Any baggage associated with George Nader . . . including but not limited to any check baggage associated with George Nader on flight EF 231 as well as any carry-on baggage, including but not limited to any briefcase, satchel, or duffel bag." The items to be seized

included “Any electronic devices capable of storing, transmitting, or receiving information, including but not limited to: Cellular telephone, Tablet, Laptop”

42. On January 17, 2018, NADER departed Dubai, United Arab Emirates on a direct flight aboard Emirates Airlines Flight 231 and arrived the same day at Washington-Dulles International Airport in Dulles, Virginia. Washington-Dulles International Airport is located in the Eastern District of Virginia.

43. Upon arrival at Washington-Dulles International Airport, NADER declared to an agent from the United States Customs and Border Protection he was in possession of three iPhones. NADER was later voluntarily interviewed by FBI agents regarding a matter unrelated to child pornography. At the conclusion of the interview, NADER was informed of the existence of the search warrant issued by this Court (1:18-SW-30) and the three iPhones were subsequently seized. The iPhones seized from NADER were later specifically identified as:

- a. iPhone 5 with serial number F2NJQ55RDTTN;
- b. iPhone 6 with serial number FK1QLB5PGRYD; and
- c. iPhone 7 with serial number F2LSD2XFHFY4.

44. On January 17, 2018, Search Warrant 1:18-SC-00114 was sworn out in the United States District Court for the District of Columbia and signed by Chief U.S. District Court Judge Beryl A. Howell. The attachments to the search warrant specified the property to be searched as “iPhone 5 with serial number F2NJQ55RDTTN, iPhone 6 with serial number FK1QLB5PGRYD, iPhone 6+ with serial number F2LSD2XFHFY4.”

45. On January 18, 2018, an order was filed with the United States District Court for the District of Columbia to correct the identification of the iPhone with serial number F2LSD2XFHFY4 to properly reflect it as an iPhone 7.

46. The three iPhones seized from NADER were then forensically processed pursuant to the search warrant for a matter not involving child pornography. At the completion of the forensic processing, the digital forensic files derived from iPhone 7 with serial number F2LSD2XFHFY4 ("IPHONE 7 FILES") were made available to the case agent in that other matter for review using a forensic software package specifically designed to allow investigators to review material without risk of changing or altering the evidence.

47. On February 12, 2018, the case agent for that other matter conducted an initial review of the IPHONE 7 FILES for evidence unrelated to child pornography. During that review, the case agent in that other matter uncovered multiple files which appeared to contain child pornography. The potential child pornography matter was subsequently referred to my office, and the case was assigned to your Affiant.

48. On March 5, 2018, the IPHONE 7 FILES were saved to a Seagate Hard Drive Model ST3750640AS with serial Number 5QD502SH. On March 16, 2018, Search Warrant 1:18-SW-154 was sworn out in the United States District Court for the Eastern District of Virginia and signed by US Magistrate Judge John F. Anderson. The attachments to the search warrant specified the property to be searched as "digital forensic files derived from the iPhone 7 with serial number F2LSD2XFHFY4 seized from George Aref Nader on January 17, 2018 currently located on a Seagate Hard Drive Model ST3750640AS with serial Number 5QD502SH that is in the custody of the Federal Bureau of Investigation in its Northern Virginia Resident Office, 9325 Discovery Boulevard, Manassas, Virginia 20109." The items to be seized included, but were not limited to, fruits, evidence, and instrumentalities of "child pornography and child erotica."

49. Pursuant to the search warrant, your Affiant conducted a review of the IPHONE 7 FILES located on a Seagate Hard Drive Model ST3750640AS with serial Number 5QD502SH. During that review, your Affiant identified the Apple ID for the iPhone 7 with serial number F2LSD2XFHFY4 as george.nadirs@gmail.com.

50. Also during that review, your Affiant located a number of files that appear to be visual depictions of minors engaged in sexually explicit conduct, including:

- a. Video #1: The video starts with two adult females and then cuts to a prepubescent boy, approximately 7 years old, who is wearing a thawb (an ankle-length Arab garment, usually with long sleeves, similar to a robe, kaftan or tunic). The boy lifts up the thawb exposing his penis. The boy then grabs his penis and shakes it. The boy is laughing as he does this and then drops the thawb over his privates. The video then cuts to an older male. The video has Arabic conversation from the adult females, child, and adult male. The video is 12 seconds in length.
- b. Video #2: The video starts with a young boy, approximately three years old, sitting on the floor with a small mechanical toy bunny that appears to knobbing up and down up against the boy's penis. An adult removes the toy and exposes the boy's penis. The boy reacts angrily and cries. The video is 4 seconds in length.
- c. Video #3: The video is an extended and reedited version of Video #2. The video starts with a boy, approximately three years old, sitting on the floor with a small mechanical toy bunny that appears to knobbing up and down up against the boy's penis. An adult removes the toy and exposes the boy's penis. The child reacts angrily and cries. The portion of the video when the adult removes the toy,

exposing the boy's penis causing him to react angrily and cry is repeated twice over. The video is approximately 13 seconds in length.

- d. Video #4: The video centers on a boy approximately thirteen (13) to fourteen (14) years old seated on a wood plank floor naked from the waist down. A goat is lying before him with all four legs tied. The boy appears to penetrate the goat from behind with his penis. The goat reacts and makes noise each time the boy thrusts. The boy looks at the camera and smiles. The video is 30 seconds in length.
- e. Video #5: The video centers on a boy approximately three (3) to four (4) years old in a farmyard naked from the waist down. Baby goats surround him. The boy looks at the camera before moving a few steps away. The baby goats follow. A hand from off screen reaches into frame and lifts the boy's shirt. The baby goats move in and suck on his penis. The boy looks at the camera. Laughing is heard. The video is 32 seconds in length.
- f. Video #6: The video centers on a boy approximately four (4) to six (6) years old seated in a classroom with other children. The boy has the front of his pants pulled down and is masturbating. A voice calls to the boy, who turns to the camera before letting go of his penis and pulling up his pants. The video is 3 seconds in length.
- g. Video #7: The video centers on three boys between the ages of six (6) and eight (8) years of age standing naked on a stage. Music plays throughout the video. Individual children approach the boys, touching the genitals of each in turn, make a gesture, and then walk away. The video is 30 seconds in length.

- h. Video #8: The video centers on a boy approximately three (3) to four (4) years old in a chicken coop naked from the waist down. The boy holds a bucket on this head while chickens surround him. After a few seconds one of the chickens pecks at the boy's penis. He cries out in pain and is let out of the chicken coop by the camera operator. The camera follows the boy. The camera operator speaks to the boy in a language other than English and films his tears. The video is 30 seconds in length.
- i. Video #9: The video centers on a boy approximately three (3) years old. The boy is seated, wearing a shirt but no pants. The boy holds a pair of pliers pointed at his genitals. Voices are heard speaking in a language other than English. The boy snaps the pliers closed on his own genitals and cries out in pain. The voices laugh. The video is 6 seconds in length.
- j. Video #10: The video centers on the nude buttocks of a boy approximately two (2) to three (3) years old. The boy is lying down on his chest. What appears to be a number pad and buttons are drawn in black ink on the boy's buttocks. A voice speaks in a language other than English and a finger presses the numbers and buttons as if the boy were an Automated Teller Machine. The boy spreads his legs and currency is removed from under the boy's penis. A child's face appears, laughing. The video is 9 seconds in length.
- k. Video #11: The video centers on a boy approximately three (3) to four (4) years old seated on a couch sharing a meal on a low table with older people. The boy reaches for something from the table and is quickly pushed onto his back on the couch. The crotch of the boy's pants splits open revealing his penis. The child

begins to cry and urinates all over the food on the table. The older people react.

The video is 6 seconds in length.

1. Video #12: The video is an extended and reedited version of Video #11. The video centers on a boy approximately three (3) to four (4) years old seated on a couch sharing a meal on a low table with older people. The boy reaches for something from the table and is quickly pushed onto his back on the couch. The crotch of the boy's pants splits open revealing his penis. The child begins to cry and urinates all over the food on the table. The older people react. The video changes to black and white and proceeds in slow motion with singing in a language other than English. The reedited portion of the video when the boy's pants split revealing his penis, he cries, and urinates all over the food on the table plays twice. The video is 16 seconds in length.

51. On March 29, 2018, the digital contents of iPhone 5 with serial number F2NJQ55RDTTN ("IPHONE 5 FILES") and iPhone 6 with serial number FK1QLB5PGRYD ("IPHONE 6 FILES") were saved to a Western Digital hard Drive with serial Number WCAYUK289060. On April 3, 2018, Search Warrant 1:18-SW-154 was sworn out in the United States District Court for the Eastern District of Virginia and signed by U.S. Magistrate Judge Michael S. Nachmanoff. The attachments to the search warrant specified the property to be searched as "digital forensic files derived from the Apple iPhone 5 with Serial Number F2NJQ55RDTTN and Apple iPhone 6 with Serial Number FK1QLB5PGRYD seized from George Aref Nader on January 17, 2018 by the FBI (the "SUBJECT FILES") . . . currently located on a Western Digital hard drive Model WD1600AAJS with Serial Number WCAYUK289060 marked "HQQ000437" that is in the custody of the Federal Bureau of

Investigation at its Northern Virginia Resident Agency, 9325 Discovery Boulevard, Manassas, Virginia 20109.” The items to be seized included, but were not limited to, fruits, evidence, and instrumentalities of “child pornography and child erotica.”

52. Pursuant to the search warrant, your Affiant conducted a review of the IPHONE 5 FILES and IPHONE 6 FILES located on a Western Digital hard Drive with serial Number WCAYUK289060. During that review, your Affiant identified the Apple ID for the iPhone 5 with serial number F2Njq55RDttn as george.nadirs@gmail.com. Also during that review, your Affiant identified the Apple ID for the iPhone 6 with serial number FK1QLB5PGRYD as george.nadirs@gmail.com.

53. Legal process was served on Google, Inc., in reference to the george.nadirs@gmail.com email address, and in response, Google, Inc., identified the name associated with the account as “George Nadir”.

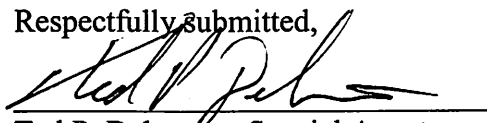
CONCLUSION

54. Based upon the above information, I respectfully submit there is probable cause to believe that information associated with the accounts described in Attachment A constitute/contain the fruits, evidence, instrumentalities and contraband of child pornography violation of the statutes described herein and as described in Attachment B.

55. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(I).

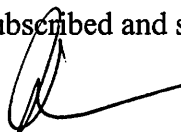
56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,


Ted P. Delacourt, Special Agent
Federal Bureau of Investigation

Approved by: AUSA Laura Fong

Subscribed and sworn to before me on, July 2, 2018


Theresa Carroll Buchanan
United States Magistrate Judge

The Honorable Theresa C. Buchanan
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE ITEMS TO BE SEARCHED

This warrant applies to information associated with the account
george.nadirs@gmail.com which is stored at premises owned, maintained, controlled, or
operated by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway
Mountain View, CA 94043.

ATTACHMENT B

Items to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A:

- a. The contents of all e-mails stored in the accounts (including attachments), including copies of e-mails sent to and from the accounts, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. Any deleted emails, including any information described in subparagraph “a,” above;
- c. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, accounts’ status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. All records or other information stored by the accounts, including but not limited to , push tokens, chat logs, address books, contact and buddy lists, calendar data, pictures, videos and files;
- e. The content of any and all cloud storage accounts;

- f. All records pertaining to Google Voice transactions/calls;
- g. All records pertaining to communications between Google and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1) and (b)(1) (transportation of visual depictions of minors engaged in sexually explicit conduct); 2252(a)(2) and (b)(1) (receipt and distribution of visual depictions of minors engaged in sexually explicit conduct); 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 2252A(a)(1) and (b)(1) (transportation of child pornography); 2252A(a)(2)(A) and (b)(1) (distribution and receipt of child pornography); and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Any and all data, records, communications or information reflecting evidence, fruits, instrumentalities, and contraband of the crimes listed above;
- b. Credit card and other financial information including but not limited to bills and payment records;
- c. Evidence of who used, owned, or controlled the accounts or identifiers listed on Attachment A;
- d. Evidence of the times the accounts or identifiers listed on Attachment A was used;

- e. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.